

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)) Case No. 21-1047M(NJ)
Apple iPhone seized from Titus Davis by Kenosha) Matter No.: 2021R00411
PD, inventoried as Item #12, Case)
#2021-00057896, currently located at Kenosha PD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A. Over which the Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 1/5/2022 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____

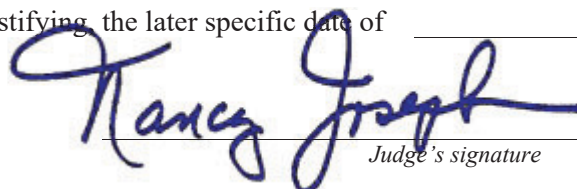
Honorable Nancy Joseph

(United States Magistrate Judge)

☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☒ for 30 days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 12/22/2021 @ 4:37 p.m.



Judge's signature

City and state: Milwaukee, Wisconsin

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

The property to be searched is an Apple iPhone with a cracked screen that was seized from Titus DAVIS by the Kenosha Police Department on November 2, 2021. The Apple iPhone was inventoried as Item #12 under Kenosha Police Department case #2021-00057896. The Apple iPhone is currently located at the Kenosha Police Department, 1000 55th Street, Kenosha, Wisconsin.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to a violation of Title 18, United States Code, section 844(i), including:

- a. All audio and video files;
- b. All voicemail and call records;
- c. All text messages;
- d. All social media sites used and applications for social media sites;
- e. All internet activity;
- f. All location data;
- g. Any information recording DAVIS' vendetta against residents of 2830 20th Avenue, Kenosha, Wisconsin;

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet Protocol address to communicate, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including

any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*

Case No. 21-1047M(NJ)

Apple iPhone seized from Titus Davis by Kenosha PD,
inventoried as Item #12, Case #2021-00057896,
currently located at Kenosha PD**Matter No.: 2021R00411****APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A. Over which the Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 844(i)

Arson;

Offense Description

The application is based on these facts:

See attached affidavit for additional offense description(s).

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of 30 days *(give exact ending date if more than 30 days)*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Digitally signed by RICKY HANKINS
DN: c=US, o=U.S. Government, ou=Dept of
Justice, ou=ATF, cn=RICKY HANKINS,
0.9.2342.19200300.100.1.1=15001001699456
Date: 2021.12.22 14:08:38 -0500

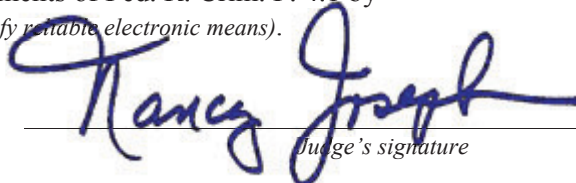
Applicant's signature

ATF SA Rick Hankins

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ *(specify reliable electronic means)*.

Date: 12/22/2021



Judge's signature

City and state: Milwaukee, Wisconsin

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Rick Hankins, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent of the United States Justice Department, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), currently assigned to the Milwaukee Field Office. I have been so employed since April 2003. My duties as a Special Agent with ATF include investigating alleged violations of the federal firearms, explosives, and arson statutes.

3. I have completed approximately 26 weeks of training at the Federal Law Enforcement Training Center (Glynco, Georgia), as well as the ATF National Academy. That training included various legal courses related to Constitutional Law as well as search and seizure authority. Additionally, I have received training on how to conduct various tasks associated with criminal investigations, such as: interviewing, surveillance, and evidence collection.

4. In addition to my duties as a criminal investigator, I am also an ATF Certified Fire Investigator (CFI). As an ATF CFI, I am tasked with providing expert opinions as to the origin and cause of fires. I obtained the ATF CFI certification in 2009 following a two-year training program that centered on various fire science topics including, but not limited to: chemistry, fire dynamics, and building construction. The two-year ATF CFI certification program consisted of college courses, written exams, research papers, reading assignments, practical training exercises, and test burns of various materials. I am re-certified annually as an ATF CFI. To date, I have

participated in over 285 fire scene examinations and have testified as an expert. Additionally, I have been certified as a fire investigator by the International Association of Arson Investigators since June 2011. I have received over 1,400 class hours of fire related training. Furthermore, I have been an instructor regarding fire related topics on multiple occasions for the following agencies and institutions: The National Fire Academy (FEMA), International Association of Arson Investigators Chapter 25, Waukesha County Technical College, and Blackhawk Technical College. I have also participated in over 200 live fire training exercises, where I started training fires and observed fire growth and development. Finally, I was a full-time instructor at the ATF National Academy from August 2015 – August 2016, where I taught several topics during Special Agent Basic Training for new ATF recruits. Specifically, I was a primary instructor for the arson block of training at the ATF Academy.

5. Through my experience and training as a firearm and arson investigator, I am aware that electronic devices, such as cellphones, can be used to store and save audio, video, and text files that can link to a variety of criminal activity. I am also aware that smart cellphones are capable of capturing location history for the device.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. The property to be searched is an Apple iPhone with a cracked screen that was seized from Titus DAVIS by the Kenosha Police Department on November 2, 2021. The Apple iPhone was inventoried as Item #12 under Kenosha Police Department case #2021-00057896. The Apple iPhone is currently located at the Kenosha Police Department, 1000 55th Street, Kenosha, Wisconsin.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B. The federal violation is related to arson, Title 18, United States Code, section 844(i).

PROBABLE CAUSE

8. On October 20, 2021, at approximately 8:35 p.m., fire caused substantial damage to an occupied residential rental property located at 4830 20th Avenue in Kenosha, Wisconsin. The structure included a lower unit and upper unit. The property affects interstate commerce because of its status as rental property.

9. Kenosha Police and Fire Department (KPD and KFD) investigators examined the fire scene and determined the fire originated on the upper landing of an exterior staircase that provided access to the upper unit.

10. Investigators made entry into the upper unit for public safety and observed narcotics in plain view.

11. Investigators further obtained surveillance video from a separate residence located within close proximity to 4830 20th Avenue that depicted the following: On October 20, 2021, at approximately 8:16 p.m., a light-colored Hyundai Santa Fe arrived at 4830 20th Avenue and parked in the street. A passenger exited the SUV and approached the front door of 4830 20th Avenue. Moments later, the passenger returned to the vehicle. At approximately 8:32 p.m., the driver of the SUV exited the vehicle and retrieved what appeared to be a gas can from the rear hatch of the SUV. The driver then approached the area of the exterior staircase that provided access to the upper unit at 4830 20th Avenue. At approximately 8:34 p.m., there was a bright flash of fire in/near the staircase, as the driver of the vehicle was seen carrying something on fire and stomping on it. The driver then returned to the SUV and subsequently left the area.

12. During their canvas of the neighborhood, investigators spoke to a witness who identified the passenger of the suspect SUV as “junior” and stated “junior” was with an individual named “Titus.” This neighborhood witness also provided the location of “junior’s” residence on 20th Avenue. Investigators were able to use “junior’s” location and the name “Titus” to search law enforcement records for police contacts and vehicle records. Investigators were subsequently able to identify “Titus Davis” who was known to drive and listed as the registered owner of a silver 2003 Hyundai Santa Fe SUV bearing Wisconsin registration plate AHX4701. Investigators determined Davis’ known vehicle is consistent with the image of the suspect vehicle in the above-described surveillance video.

13. On November 2, 2021, at approximately 6:58 p.m., KPD Police Officer Joshua Fikejs observed the above-described Hyundai Sante Fe parked in a parking lot at 1821 Washington Road, Kenosha, Wisconsin. Officer Fikejs approached the vehicle and observed it was occupied by Titus DAVIS in the driver’s seat and R.S. in the passenger seat. Due to the open arson investigation and KPD’s suspect alert, PO Fikejs asked DAVIS if DAVIS would be willing to voluntarily go with PO Fikejs to the KPD Detective Bureau to talk to KPD Detective Daniel Wienke regarding KPD’s arson investigation. DAVIS stated he was willing to go with PO Fikejs to KPD and talk to investigators.

14. On November 2, 2021, DAVIS engaged in a voluntary, non-custodial interview with KPD Detective Wienke. During the interview, DAVIS’s cell phone was displayed on the interview table and DAVIS showed Detective Wienke a phone number of an individual potentially connected to the arson location. Detective Wienke then observed significant bandages on DAVIS’ hands. The interview subsequently addressed DAVIS’ bandaged hands and DAVIS eventually

agreed to show Detective Wienke the wounds covered by the bandages. Detective Wienke observed what appeared to be burn marks / wounds.

15. After observing DAVIS wounds, Detective Wienke confronted DAVIS with the inconsistencies in his prior explanation(s) for the bandages. DAVIS told Detective Wienke he would tell the Detective what happened after DAVIS had the opportunity to speak with R.S. and his “aunt.” Detective Wienke then went into the KPD lobby where R.S. and DAVIS’ “aunt” were waiting for DAVIS. Detective Wienke spoke to DAVIS’ “aunt.” DAVIS’ “aunt” stated that DAVIS came to her house a “few weeks ago” and told her daughter that he burned his face and hands. The “aunt” stated her daughter applied bandages to DAVIS’ hands and then took DAVIS to a hospital for treatment.

16. After speaking to R.S. and DAVIS’ “aunt,” Detective Wienke returned to DAVIS’ interview room and notified DAVIS that he was no longer free to leave. Detective Wienke read the “Constitutional Rights form” (Miranda warning) to DAVIS. DAVIS waived his rights and agreed to make a statement. DAVIS stated that on the night of October 20, 2021, while under the influence, DAVIS went to 4830 20th Avenue (upper unit) because he was upset with the resident, J.M. According to DAVIS, J.M. and his/her associates robbed DAVIS on previous date. DAVIS then stated he should not have done it (alluding to the fire).

17. While taking DAVIS into custody, KPD officers took custody of DAVIS’ cell phone, an Apple iPhone, which was inventoried as Item #12 under Kenosha Police Department case #2021-00057896. DAVIS’ Apple iPhone is currently located at the Kenosha Police Department, 1000 55th Street, Kenosha, Wisconsin.

18. Based on the above-described facts, ATF previously obtained the following Federal search warrant for Davis’ above-described cell phone: #21-M-528, which was signed by United

States Magistrate Judge Stephen Dries on November 22, 2021. Said search warrant authorized the examination of the aforementioned cellphone (Item #12). However, the forensic examiner at the Kenosha Police Department erroneously extracted data from the wrong cellphone (Item #8), which was also in their inventory for this same case.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed

and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- d. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address

so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Based on my training, experience, and research, I know that the Devices have capabilities that allow it to serve as a wireless telephone, digital camera and video recorder, portable media player, internet web browser, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been

downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
 - c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
 - d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence

of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

The property to be searched is an Apple iPhone with a cracked screen that was seized from Titus DAVIS by the Kenosha Police Department on November 2, 2021. The Apple iPhone was inventoried as Item #12 under Kenosha Police Department case #2021-00057896. The Apple iPhone is currently located at the Kenosha Police Department, 1000 55th Street, Kenosha, Wisconsin.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to a violation of Title 18, United States Code, section 844(i), including:

- a. All audio and video files;
- b. All voicemail and call records;
- c. All text messages;
- d. All social media sites used and applications for social media sites;
- e. All internet activity;
- f. All location data;
- g. Any information recording DAVIS' vendetta against residents of 2830 20th Avenue, Kenosha, Wisconsin;

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet Protocol address to communicate, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including

any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.